REMARKS

The Applicants and the undersigned thank Examiner Gurshman for his careful review of this application. Claims 1, 3-14, 16-31, and 33-34, and 36-41 have been rejected by the Examiner. Upon entry of this amendment, Claims 2, 15, 32, and 35 have been cancelled, and Claims 1, 3-14, 16-31, and 33-34, and 36-41 remain pending in this application. The independent claims are Claims 1, 14, 18, 22, 26, and 31.

Consideration of the present application is respectfully requested in light of the above claim amendments to the application, the telephonic interview, and in view of the following remarks.

Claim Rejections Under 35 U.S.C. § 112, second paragraph

The Examiner rejected Claim 31 under 35 U.S.C. § 112, second paragraph as failing to particularly point out and distinctly claiming the subject matter which the Applicants regard as the invention. Specifically, the Examiner believes that the term "substantially minimized" is a relative term and renders this claim as indefinite.

The Applicants appreciate the Examiner's helpful comments. The Applicants have cancelled this phrase from Claim 31 to advance prosecution of this patent application. Reconsideration and withdrawal of this rejection are respectfully requested.

Claim Rejections Under 35 U.S.C. § 103

The Examiner rejected Claims 1, 3-14, 16-31, and 33-41as being obvious over U.S. Pat. No. 6,453,345 issued in the name of Trcka et al. (hereinafter, the "Trcka reference") in view of U.S. Pat. No. 5,557,742 issued in the name of Smaha et al. (hereinafter, the "Smaha reference").

The Applicants respectfully offer remarks to traverse these pending rejections. The Applicants will address each independent claim separately as the Applicants believes that each independent claim is separately patentable over the prior art of record.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Trcka and Smaha references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) receiving raw computer events with a fusion engine from one or more data sources, (2) each data source comprising an intrusion detector that assigns a priority status to each raw computer event, (3) each raw computer event comprising one of suspicious computer activity and a computer attack; (4) classifying the raw computer events with the fusion engine by assigning each raw computer event an event type parameter; (5) storing the raw computer events; (6) comparing each raw computer event and its type with computer environment information stored in a knowledge-based database; (7) assigning context parameters to each raw computer event based on the comparison of a respective computer event and its type with the computer environment information; (8) determining if a priority status of each raw computer event should be adjusted based on its assigned context parameters; (9) adjusting a priority status or leaving a priority status of a raw computer event in tact based on the determination step; (10) identifying one or more relationships between two or more raw computer events by using rules associated with the event type parameters and that are executed with the fusion engine (11) to determine if the two or more raw computer events are part of a larger computer attack; (12) in response to identifying one or more relationships between two or more raw computer events, generating a mature correlation event message; and (13) displaying one or more mature correlation event messages on one or more consoles that describe relationships between raw computer events, as recited in amended independent Claim 1.

The Trcka Reference

The Trcka reference describes a network security and surveillance system that passively generates an archival recording of raw, bi-directional computer traffic that is present on a computer network 30 as illustrated in Figure 1 of the reference. The Trcka system includes a monitoring computer 34 that is connected to the computer network 30 at a network monitoring point 36. See Figure 1 of the Trcka system reproduced below.

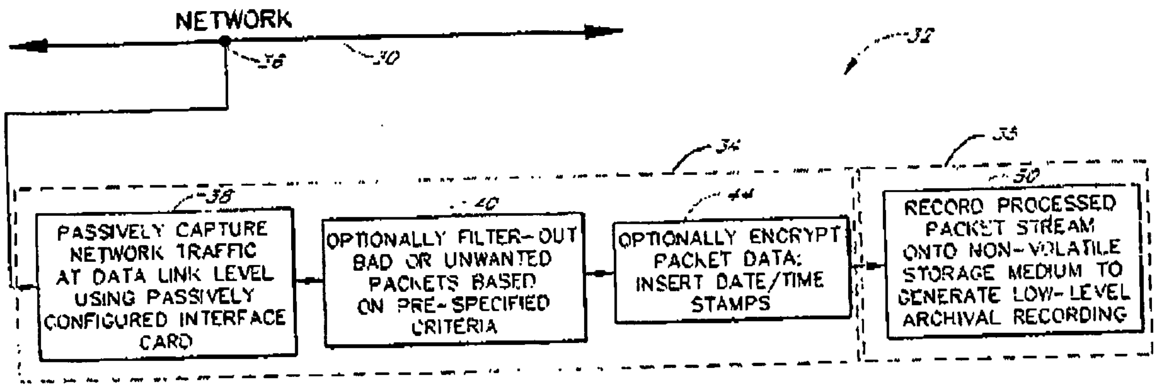
NETWORK
36
30
32
34
35
38
40
44
50
PASSIVELY CAPTURE NETWORK TRAFFIC AT DATA LINK LEVEL USING PASSIVELY CONFIGURED INTERFACE CARD
OPTIONALLY FILTER-OUT BAD OR UNWANTED PACKETS BASED ON PRE-SPECIFIED CRITERIA
OPTIONALLY ENCRYPT PACKET DATA; INSERT DATE/TIME STAMPS
RECORD PROCESSED PACKET STREAM ONTO NON-VOLATILE STORAGE MEDIUM TO GENERATE LOW-LEVEL ARCHIVAL RECORDING

FIG. 1

The monitoring computer 34 of the Trcka reference includes an interface card 38 for passively capturing network traffic a the data link level. The monitoring computer 34 employs a filter 40 to remove bad or unwanted packets based on pre-specified criteria. After bad or unwanted packets are removed, the computer 34 has an encryption device 44 that can encrypt the packet data as well as insert date and time stamps.

Once data and time stamps have been inserted, the computer 34 has a non-volatile storage medium 50 that can maintain a complete replica of all valid network traffic. See the Trcka reference, column 5, lines 25-45; column 6, lines 40-68; and in column 7, lines 14-42.

Opposite to the monitoring computer 34 of the Trcka reference, the invention described by amended independent Claim 1 provides the receiving of raw computer events with a fusion engine from one or more data sources wherein each data source comprises an intrusion detector and wherein each raw computer event comprises one of suspicious computer activity and a computer attack;. The fusion engine as described by amended independent Claim 1 identifies one or more relationships between two or more raw computer events by determining if the two or more raw computer events are part of a larger computer attack. The Trcka reference does not provide any teaching of monitoring raw computer events from multiple intrusion detectors and determining if two or more raw computer events are part of a larger attack, as recited in amended independent Claim 1 in combination with the other claim elements.

Further, the Trcka reference does not provide any teaching of determining if a priority status of each raw computer event should be adjusted based on its assigned context parameters. The Trcka reference also does not identify one or more relationships between two or more raw computer events by using rules associated with the event type parameters and that are executed with the fusion engine. The Examiner admits that the Trcka reference does not provide any teaching of determining if two or more raw computer events are part of a larger computer attack.

The Smaha Reference

The Examiner also admits that the Trcka reference fails to provide any teaching of generating one or more correlation event messages. To make up for this deficiency and the determination of whether two or more raw computer events are part of a larger computer attack, the Examiner relies upon the Smaha reference.

Specifically, the Examiner refers the Applicants to Figure 5a of the Smaha reference that illustrates comparing data structures with signature structures. See Figure 5a of the Smaha reference reproduced below.

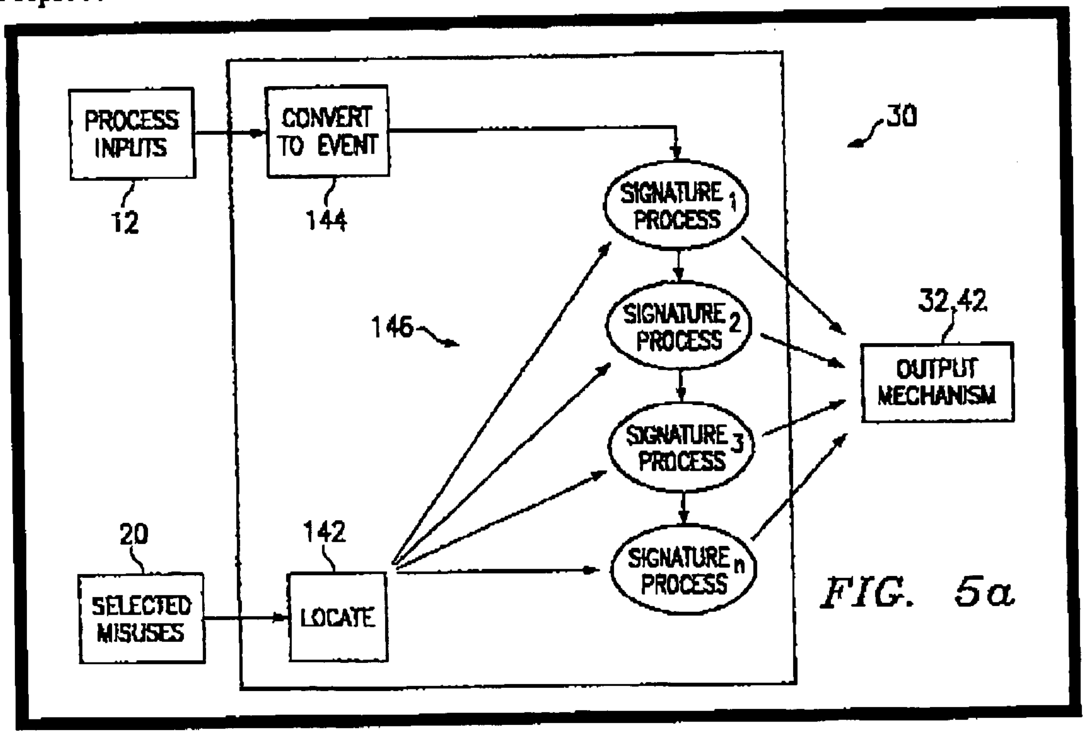

FIG. 5a

The Smaha reference describes the operation of misuse engine 30 in which the misuse engine 30 receives inputs from input mechanism 20 of selected misuses and from process inputs mechanism 12. Misuse engine 30 results may go to various output mechanisms, including, for example, output signal mechanism 32 and output report mechanism 42. A first step is to locate the selected misuses and define a processing stream. For this purpose, locate mechanism 142 of Figure 5a operates as part of misuse engine 30 to receive as inputs from selected misuses input mechanism 20 and uses signature data structure 108. Smaha reference, column 9, lines 30-42.

For each selected misuse, detection system 10 uses index 110 of signature data structure 108 to locate from signature data structure 108 the initial state 112, and the sets of transition functions 114. In addition, index 110 defines appropriate sets of states 116, as well as end state 118. Thus, for each misuse there is an initial state 112. Smaha reference, column 9, lines 43-55.

The sets of states 116 that the misuse engine 30 locates from data structure 108 may be as empty or large as necessary to represent all the states in the sequence of actions which result in the misuse. Any set of events may also include the initial event 112 or events in previous sets. The effect of transitioning to the initial state is to reset the sequence of actions to the initial state. With the misuse engine 30, there is no requirement of time ordering or directional processing between transition functions and states. However, signature data structure 108 may use temporally-defined transitions. The Smaha reference explains that this is materially from different expert systems which cannot support temporally-ordered or temporally-defined transitions. The combination of unlimited transition functions and states also allows the representation of any pattern of events. Smaha reference, column 9, lines 55-62.

The misuse engine 30 of the Smaha reference also converts the process inputs 12 into events at convert to event step or mechanism 144. Convert to event mechanism 144 processes the process inputs according to the method defined in Figure 2 and generates events. This conversion occurs continuously until the processing is terminated by either exhausting the audit trail records or by the method being interrupted. Each event generated by step 144 is passed through each signature process which collectively use reference manual 146.

Principle Operation for Smaha Reference

The Smaha reference explains and emphasizes that its system with the misuse engine 30 eliminates the need for expert system programmers to enter knowledge database rules in its system. Smaha reference, column 3, lines 12-15; lines 25-26; column 4, lines 1-2; and column 11, lines 54-60. Meanwhile, the Examiner refers to the Applicants to reference numeral 96 of Figure 3 of the Trcka reference for a teaching of a rule data base for determining if relationships exist between two or more events. Further, each independent claim pending in this patent application recite the use of rules either to determine if the two or more raw computer events are part of a larger computer attack or generating a mature correlation event message in response to each successful application of a rule.

One of ordinary skill in the art recognizes that the proposed modification by the Examiner in which the Trcka reference that uses rules is combined with the Smaha reference changes the principle operation of the Smaha reference. The Applicant further submits that MPEP § 2143.01, subsection VI (Rev. 3, August 2005), states the following:

> "If the proposed modification or a combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)."

The proposed modification in which the Examiner combines the rules-based Trcka reference with the signature-based Smaha reference would change the principle of operation of the Smaha reference because the Smaha explicitly and expressly teaches away from using any rules in its system. Therefore, one of ordinary skill in the art would not combine the references in a manner as suggested by the Examiner.

Even if the Examiner maintains the position that these two references are combinable, the Applicants further submit that the Smaha-Trcka combination proposed by the Examiner does not provide any teaching of adjusting a priority parameter assigned to each raw computer event if one or more conditions are met as described by amended independent Claim 1.

Conclusion Regarding Independent Claim 1

In light of the differences between Claim 1 and the Trcka and Smaha references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of this rejection of Claim 1 are respectfully requested.

Independent Claim 14

The rejection of Claim 14 is respectfully traversed. It is respectfully submitted that the Trcka and Smaha references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) receiving a plurality of raw computer events with a fusion engine from one or more intrusion detectors that assign a priority parameter to each raw computer event, (2) each raw computer event having a first set of parameters and comprising one of suspicious computer activity and a computer attack; (3) creating raw computer event storage areas based upon information received from a raw computer event classification database; (4) storing each event in an event storage area based upon an event type parameter; (5) comparing each raw computer event to data contained in a context database with the fusion engine to determine if the two or more raw computer events are part of a larger computer attack; (6) adjusting a priority parameter or leaving the priority parameter in tact for each raw computer event in response to the comparison to the context database; (7) associating each raw computer event with one or more correlation events; (8) applying one or more rules corresponding with the event type parameters to each raw computer event based upon the correlation event associations; and (9) generating a mature correlation event message in response to each successful application of a rule, as recited in amended independent Claim 14.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address a combination of elements that includes rules and evaluating priority parameters of raw computer events, as recited in amended independent Claim 14.

In light of the differences between Claim 14 and the Trcka and Smaha references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 14. Accordingly, reconsideration and withdrawal of this rejection of Claim 14 are respectfully requested.

Independent Claim 18

The rejection of Claim 18 is respectfully traversed. It is respectfully submitted that the Trcka and Smaha references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) a plurality of data sources comprising intrusion detectors that assign a priority parameter to raw computer events; (2) an event collector linked to the plurality of data sources; (3) a fusion engine linked to the event collector, (4) said fusion engine identifying relationships between two or more raw computer events generated by the data sources and (5) adjusting each priority parameter if one or more conditions are met, (6) the fusion engine using rules associated with event type parameters assigned to each raw computer event (7) to determine if the two or more raw computer events are part of a larger computer attack, (8) each raw computer event comprising one of suspicious computer activity and a computer attack; and (9) a console linked to the event collector for displaying any output generated by the fusion engine, as recited in amended independent Claim 21.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address a combination of elements that includes rules and evaluating priority parameters of raw computer events, as recited in amended independent Claim 18.

In light of the differences between Claim 18 and the Trcka and Smaha references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 18. Accordingly, reconsideration and withdrawal of this rejection of Claim 18 are respectfully requested.

Independent Claim 22

The rejection of Claim 22 is respectfully traversed. It is respectfully submitted that the Trcka and Smaha references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) a controller; (2) an event reader for receiving raw computer events from intrusion detectors that assign a priority parameter to each raw computer event, (3) each raw computer event comprising one of suspicious computer activity and a computer attack; (3) a classifier linked to the event reader for classifying the received raw computer events; (4) a raw computer event classification database linked to the classifier; (5) a context based risk-adjustment processor linked to the classifier, for adjusting the priority parameters of raw computer events; (6) a context database linked to the context based risk-adjustment processor for providing context parameters that are assigned to raw computer events and that are used by the context based risk-adjustment processor; and (7) a rule database that comprises rules (8) for identifying if one or more relationships exist between two or more events by determining if the two or more raw computer events are part of a larger computer attack, as recited in amended independent Claim 22.

Similar to the analysis independent Claim 1, neither the Trcka nor the Smaha references alone or in combination teach rules and evaluating priority parameters of raw computer events in addition to the other elements recited in amended Claim 22.

In light of the differences between Claim 22 and the Trcka and Smaha references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 22. Accordingly, reconsideration and withdrawal of this rejection of Claim 22 are respectfully requested.

Independent Claim 26

The rejection of Claim 26 is respectfully traversed. It is respectfully submitted that the Trcka and Smaha references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) receiving with a fusion engine a raw computer event having a first ranking from one or more data sources comprising intrusion detectors, (3) each raw computer event comprising one of suspicious computer activity and a computer attack; (4) classifying the raw computer event with the fusion engine (5) by assigning each raw computer event an event type parameter; (6) storing the raw computer event; (7) assigning a second ranking to the raw computer event with the fusion engine, the second ranking assesses risks of the raw computer event based upon a context of the raw computer event; (8) determining if the first ranking each raw computer event should be adjusted based on its second ranking; and (9) identifying one or more relationships between two or more raw computer events by using rules associated with event type parameters (10) to determine if the raw computer event is part of a larger computer attack, as recited in amended independent Claim 26.

Similar to the analysis independent Claim 1, neither the Trcka nor the Smaha references alone or in combination teach rules and evaluating priority parameters of raw computer events combined with the other elements recited in amended Claim 26.

In light of the differences between Claim 26 and the Trcka and Smaha references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the

Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 26. Accordingly, reconsideration and withdrawal of this rejection of Claim 26 are respectfully requested.

Independent Claim 31

The rejection of Claim 31 is respectfully traversed. It is respectfully submitted that the Trcka and Smaha references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) receiving raw computer events with a fusion engine from one or more data sources comprising intrusion detectors that assign a priority status to each raw computer event, (2) each raw computer event comprising one of suspicious computer activity and a computer attack; (2) classifying the raw computer events with the fusion engine by assigning each raw computer event an event type parameter; (4) assigning context parameters to each raw computer event based on the comparison of a respective computer event and its type parameter with computer environment information; (5) determining if a priority status of each raw computer event should be adjusted based on its context parameters; (6) grouping two or more raw computer events into a high level correlation event with the fusion engine if the two or more raw computer events are part of a larger computer attack; (7) in response to grouping the two or more raw computer events, applying one or more rules to the raw computer events; (8) generating a mature correlation event message if application of a rule is successful; and (9) displaying one or more mature correlation event messages on a console that describe relationships between raw computer events, as recited in amended independent Claim 31.

Similar to the analysis independent Claim 1, neither the Trcka nor the Smaha references alone or in combination teach rules and evaluating priority parameters of raw computer events combined with the other elements recited in amended Claim 31.

In light of the differences between Claim 31 and the Trcka and Smaha references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 31. Accordingly, reconsideration and withdrawal of this rejection of Claim 31 are respectfully requested.

Dependent Claims 3-13, 16-17, 19-21, 23-25, 27-30, and 33-34, and 36-41

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references. The Applicants also rcspcctfully submit that the recitations of these dependent claims are of patentable significance.

In view of the foregoing, the Applicants respectfully request that the Examiner withdraw the pending rejections of dependent Claims 3-13, 16-17, 19-21, 23-25, 27-30, and 33-34, and 36-41.

CONCLUSION

The foregoing is submitted as a full and complete response to the Office Action mailed on November 8, 2005. The Applicants and the undersigned thank Examiner Gurshman for consideration of these remarks. The Applicants have amended the claims and have submitted remarks to traverse rejections of Claims 1, 3-14, 16-31, and 33-34, and 36-41. The Applicants respectfully submit that the present application is in condition for allowance. Such action is hereby courteously solicited.

If the Examiner believes that there arc any issues that can be resolved by a telephone conference, or that there are any formalities that can be corrected by an Examiner's amendment, the Examiner is invited to contact the undersigned in the Atlanta Metropolitan area (404) 572-2884.

Respectfully submitted,

Steven P. Wigmore
Reg. No. 40,447

King & Spalding LLP
191 Peachtree Street, N.E.
Atlanta, Georgia 30303-1763
telephone: (404) 572.4600
K&S File No. 05456-105006